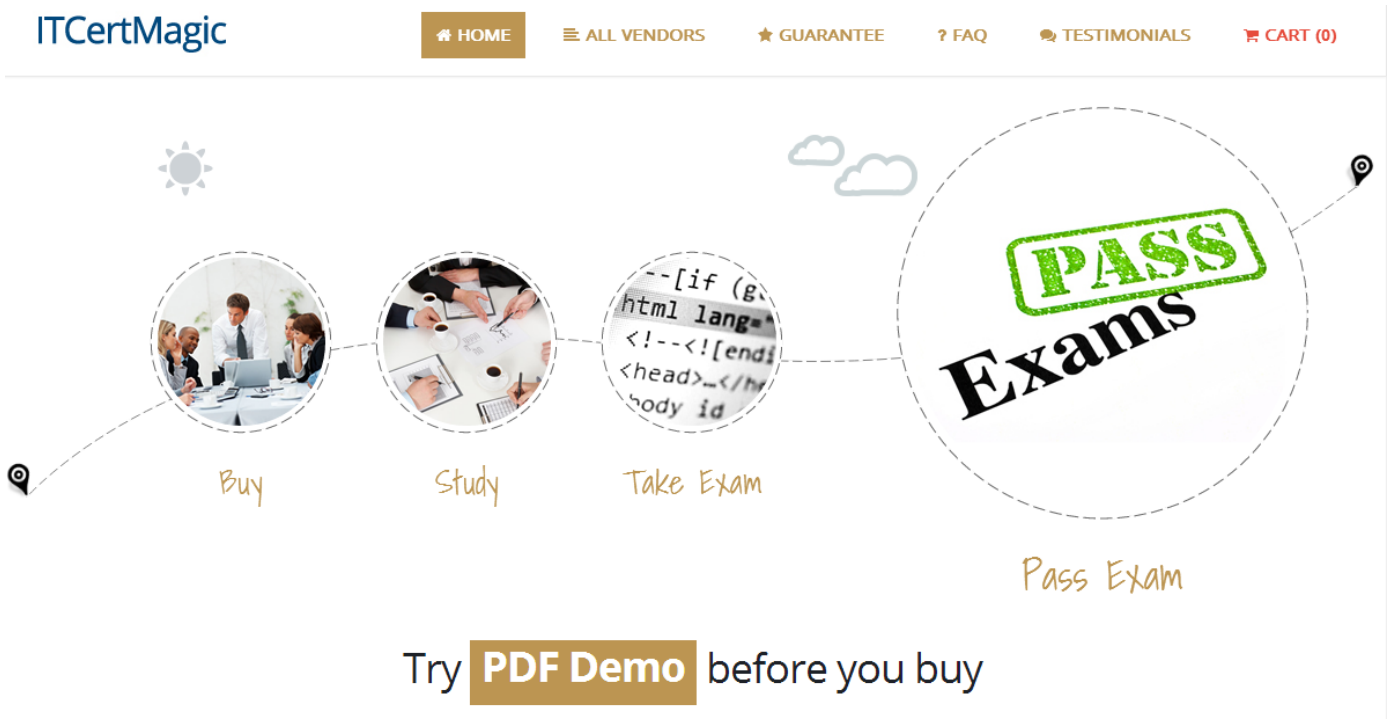
ITCertMagic



http://www.itcertmagic.com/

Pass-Guaranteed Certification Exam Questions | Exam Dumps - ITCertMagic

Exam : **C1000-162**

Title : IBM Security QRadar SIEM V7.5 Analysis

Vendor : IBM

Version : DEMO

NO.1 When you create a report, you must choose a chart type for each chart that is included in the report.
Which two (2) chart types can you include in a report?
A. Flows
B. Raw Data
C. Containers
D. Scanners
E. Log Sources
Answer: A B
Explanation:
While the options could be more clearly phrased, here's why these answers are likely correct:
* Report Content: QRadar reports visualize security data. These types fit:
* Flows: Represent network traffic patterns. Visualizing them in charts is common in reports.
* Raw Data: Often meant to refer to tabulated events/logs. This can be charted.

NO.2 What is the name of the data collection set used in QRadar that can be populated with IOCs or other external data?
A. Index set
B. Reference set
C. IOC set
D. Data set
Answer: B
* IOCs and Reference Sets: Reference sets are specifically designed to store lists of Indicators of Compromise (IOCs) like IP addresses, domain names, file hashes, etc.
* Correlation and Matching: QRadar can match events and flows against data in reference sets, triggering rules or alerts when suspicious activity is detected.

NO.3 Which statement regarding the use of the internal structured language of the QRadar database is true?
A. Use AQL to extract, filter, and perform actions on event and flow data that you extract from the Ariel database
B. Use AQL to extract, filter and manipulate event, flow and use cases data from the Ariel database
C. Use AQL to accelerate and make tuning event and flow data from the Ariel database
D. Use AQL to accelerate and make tuning event, flow and use cases data from the Ariel database
Answer: A
Explanation:
The Ariel Query Language (AQL) is the internal structured language used in QRadar for interacting with the Ariel database, which stores event and flow data. AQL allows users to perform complex queries to extract, filter, and analyze this data, enabling detailed investigations and insights into security incidents and network activity. By using AQL, analysts can tailor their queries to meet specific informational needs, making it a powerful tool for data extraction and manipulation within the QRadar environment.

NO.4 What does the logical operator != in an AQL query do?

A. Compares a property to a value and returns false if they are unequal
B. Takes a value and raises it to the specified power and returns the result
C. Sets the value on the left of the operator equal to the right
D. Compares two values and returns true if they are unequal
Answer: D
Explanation:
The logical operator != in an AQL (Ariel Query Language) query is used to compare two values and returns true if the values are unequal. This operator is a common element in various programming and query languages, and its purpose is consistent across these environments, including in IBM Security QRadar SIEM V7.5.
For instance, in an AQL query, if you are analyzing event or flow data and want to filter out records where a specific field, say username, does not equal a certain value, you could use the != operator in your query like so: SELECT * FROM events WHERE username != 'admin'. This query would return all records where the username field does not equal 'admin'.
The use of the != operator is crucial in data analysis and threat hunting within QRadar, as it allows security analysts to exclude certain data points and focus on the relevant data that might indicate security incidents or breaches.

NO.5 Events can be exported from the QRadar Log Activity tab in which file formats?
A. JSON. XML, and CSV
B. XLS and CSV
C. JSON and XML
D. XML and CSV
Answer: D
Explanation:
Events can be exported from the QRadar Log Activity tab in XML (Extensible Markup Language) or CSV (Comma-Separated Values) formats, providing flexibility in how data is extracted and used for further analysis outside of QRadar.

NO.6 AQRadar analyst can check the rule coverage of MITRE ATT&CK tactics and techniques by using Use Case Manager.
In the Use Case Manager app, how can a QRadar analyst check the offenses triggered and mapped to MITRE ATT&CK framework?
A. By navigating to "CRE Report"
B. From Offenses tab
C. By clicking on "Tuning Home"
D. By navigating to "Detected in timeframe"
Answer: D
Explanation:
To check the offenses triggered and mapped to the MITRE ATT&CK framework using the Use Case Manager app, an analyst can navigate through the Offenses tab, click on All Offenses, and then utilize the All Offenses Summary toolbar to display rules contributing to an offense. This process allows for an investigation into how offenses correlate with the MITRE ATT&CK framework. However, the exact option "Detected in timeframe" is not explicitly mentioned in the provided documentation, and the described procedure offers a broader approach to reviewing offenses and their associated rules

within the MITRE ATT&CK context.

NO.7 On the Dashboard tab in QRadar. dashboards update real-time data at what interval?
A. 1 minute
B. 3 minutes
C. 10 minutes
D. 7 minutes
Answer: A
* Dashboard Data Refresh: Most widgets on QRadar dashboards typically refresh the displayed data every minute by default.
* Customization: In some cases, you might be able to configure this refresh interval depending on the widget type.

NO.8 Which two (2) aggregation types are available for the pie chart in the Pulse app?
A. Last
B. Middle
C. Total
D. First
E. Average
Answer: C D
* Pie Chart Logic: Pie charts represent proportions of a whole.expand_more QRadar Pulse supports the following aggregations suitable for this:
* Total (Sum): Calculates the sum of a selected field's values, displaying each slice relative to the whole.
* First: Takes the first value encountered in a field, useful for categorical data to show initial distribution.

NO.9 What type of reference data collection would you use to correlate a unique key to a value?
A. Reference map
B. Reference list
C. Reference table
D. Reference set
Answer: A
Explanation:
* Understanding Reference Data Collections in QRadar: In IBM QRadar, reference data collections are used to store data that can be reused across various rules, searches, and reports. Each type of reference data collection has a specific use case and structure.
* Types of Reference Data Collections:
* Reference Map: Stores key-value pairs where each key is unique and maps to a specific value.
* Reference List: Stores a list of values without any keys.
* Reference Table: Stores multiple key-value pairs where each key can have multiple values.
* Reference Set: Stores a set of unique values without any keys.
* Use Case for Reference Map: When you need to correlate a unique key to a specific value, a reference map is the appropriate data structure. It allows for efficient lookups and associations between keys and their corresponding values.

* Reference Confirmation: According to IBM QRadar documentation, a reference map is explicitly designed to correlate unique keys to values, making it the correct choice for such requirements.
References:
* IBM QRadar documentation on reference data collections confirms the use of a reference map for correlating unique keys to values.

NO.10 Which two high level Event Categories are used by QRadar? (Choose two.)
A. Policy
B. Direction
C. Localization
D. Justification
E. Authentication
Answer: A E

NO.11 In QRadar. common rules test against what?
A. They test against incoming log source data that is processed by QRadar Event Processor
B. They test the parameters of an offense to trigger more response
C. They test against event and flow data
D. They test against incoming flow data that is processed by the QRadar Flow Processor
Answer: A
* Common Rules: The foundation of QRadar's event analysis. They operate on structured events representing activity from various log sources.
* Event Processor: Responsible for normalizing and categorizing raw log data from various sources into structured QRadar events.

NO.12 Which flow fields should be used to determine how long a session has been active on a network?
A. Start time and end time
B. Start time and storage time
C. Start time and last packet time
D. Last packet time and storage time
Answer: C

NO.13 Which two (2) options are at the top level when an analyst right-clicks on the Source IP or Destination IP that is associated with an offense at the Offense Summary?
A. Information
B. Asset Summary page
C. Navigate
D. WHOIS Lookup
E. DNS Lookup
Answer: D E
* Context Menu: Right-clicking on an IP address in the Offense Summary window offers quick
* investigation actions.
* IP-Related Tools: WHOIS and DNS Lookups are essential tools for:

* WHOIS: Retrieving IP registration information (owner, contact details, etc.). DNS: Resolving domain names associated with the IP.

NO.14 What two (2) guidelines should you follow when you define your network hierarchy?

A. Do not configure a network group with more than 15 objects.

B. Organize your systems and networks by role or similar traffic patterns.

C. Use the autoupdates feature to automatically populate the network hierarchy.

D. Import scan results into QRadar.

E. Use flow data to build the asset database.

Answer: B E

Explanation:

When defining the network hierarchy in QRadar, it is recommended to organize systems and networks by role or similar traffic patterns to differentiate network behavior effectively. Additionally, it is advised not to configure a network group with more than 15 objects to avoid difficulties in viewing detailed information for each object and to ensure efficient management of network groups.